Hello,

I had said I would provide additional information on Incident Handling and Coordination standards for this week's call. Please let me know if additional information is needed or if any other formats should be used.

The specific standardized protocols that should be used include:

SCAP: to automate the detection and supply information about the state of systems involved in an incident. This can be combined with event information to see if a vulnerability is present and if the configuration might allow for that vulnerability to be exploited. Event information may provide details on an attempt to exploit that vulnerability.

Once you have an event that moves to the state of becoming an incident, a standard format is needed to track and coordinate the incident response handling activities. A set of standards have been published via the IETF to provide this capability.

RFC5070, Incident Object Description and Exchange Format (IODEF): Provides a standard format to exchange incident information.

RFC6045, Real-time Inter-network Defense (RID): To provide a standard method to communicate incident information between entities (cloud providers, government entities, country level CSIRTS, organizations/agencies)

There are several other RFCs that provide extensions to the IODEF data model and include RFC5941 and RFC5901. The data model is easily extended to address other use cases.

There is a transport protocol defined in RFC6046, however I am not sure this will be the long-term transport yet.

I am working with the SCAP team at NIST as well as with Tom Millar at DHS who heads up US CERT in combining these protocols for a standards-based solution (all protocols are standards and are published as such). I am also the co-editor for Incident response and coordination in the ITUT effort as well as the CSA CloudCERT effort. It would be very nice to see the same set of standards used to facilitate communication across cloud providers and CERTS. IODEF is already used at country level CERTs.

Thank you,

Kathleen

Kathleen M. Moriarty
CISSP
GRC Strategy
Office of the CTO
EMC Corporation